CLAIMS:

1. (Currently Amended): A system in a message source for secure communication, comprising:

a random value generator configured to generate a random value;

a message validation code generator coupled to the random value generator and configured to generate a message validation code based on a predetermined key, a message, and the random value;

a one-time pad generator coupled to the random number generator and configured to generate a one-time pad based on the random value and the predetermined key; [[and]]

a masked message generator coupled to the one-time pad generator and configured to generate a masked message based on the one-time pad and the message, and

a transmitter configured to transmit a secure message that comprises the random value, the masked message, and the message validation code to a message target,

wherein the message target is configured to unmask the masked message to form the message and validate the message using the message validation code.

2. (Original): The system as recited in claim 1, wherein the message validation code generator employs a first one-way hash function.

3. (Original): The system as recited in claim 2, wherein the one-time pad generator employs the first one-way hash function.

4. (Original): The system as recited in claim 1, wherein the message validation code generator employs a first one-way hash function and the one-time pad generator employs a second one-way hash function.

5. (Original): The system as recited in claim 1, further comprising a protected message envelope generator coupled to the random value generator, the message validation code generator, and the masked message generator, and configured to generate a protected

message envelope based on the random value, the message validation code, and the masked message.

6. (Currently Amended): The system as recited in claim 5, ~~further comprising a~~ wherein the transmitter is coupled to the protected message envelope generator and configured to transmit the protected message envelope to [[a]] the message target.

7. (Currently Amended): A system in a message target for secure communication, comprising:

a receiver configured to receive a secure message transmitted from a message source, wherein the secure message comprises a protected message envelope;

a protected message envelope reader configured to receive [[a]] the protected message envelope and ~~generate~~ extract a random value, a masked message, and a first message validation code ~~based on~~ from the received protected message envelope, wherein the random value, the masked message, and the first message validation code are generated at the message source;

a one-time pad generator coupled to the protected message envelope reader and configured to generate a one-time pad based on the random value and a predetermined key; and

a message unmasker coupled to the one-time pad generator and protected message envelope reader, and configured to generate an unmasked message based on the one-time pad and the masked message.

8. (Original): The system as recited in claim 7, wherein the one-time pad generator employs a first one-way hash function.

9. (Original): The system as recited in claim 7, further comprising a validation module coupled to the protected message envelope reader and the message unmasker, the validation module comprising:

a message validation code generator configured to generate a second message validation code based on the predetermined key, the unmasked message, and the random value; and

a message validation code comparator coupled to the protected message envelope reader and the message validation code generator and configured to generate a validation based on the first message validation code and the second message validation code.

10. (Original): The system as recited in claim 9, wherein the validation module employs a first one-way hash function.

11. (Original): The system as recited in claim 9, wherein the validation module employs a first one-way hash function and the one-time pad generator employs a second one-way hash function.

12. (Currently Amended): A method in a message source for secure communication, comprising:

generating a random value;

generating a message validation code based on a message, the random value, a predetermined key, and a first one-way hash function;

generating a one-time pad based on the random value, the predetermined key, and a second one-way hash function; [[and]]

generating a masked message based on the message and the one-time pad; and

transmitting a secure message that comprises the random value, the masked message, and the message validation code to a message target,

wherein the message target is configured to unmask the masked message to form the message and validate the message using the message validation code.

13. (Original): The method as recited in claim 12, further comprising generating a protected message envelope based on the random value, the masked message, and the message validation code.

14. (Currently Amended): The method as recited in claim 13, ~~further comprising transmitting~~ wherein the secure message comprises the protected message envelope ~~to a target destination~~.

15. (Original): The method as recited in claim 12, wherein the first one-way hash function and the second one-way hash function are the same one-way hash function.

16. (Canceled)

17. (Canceled)

18. (Currently Amended): A method in a message target for secure communication, comprising:

receiving a secure message transmitted from a message source, wherein the secure message comprises a random value, a masked message, and a first message validation code, wherein the random value, the masked message, and the first message validation code are generated at the message source;

generating a one-time pad based on the random value, a predetermined key, and a first one-way hash function; and

generating an unmasked message based on the one-time pad and the masked message.

19. (Original): The method as recited in claim 18, further comprising:

generating a second message validation code based on the unmasked message, the random value, the predetermined key and a second one-way hash function; and

comparing the first message validation code to the second message validation code to determine a validity of the unmasked message.

20. (Original): The method as recited in claim 19, wherein the first one-way hash function and the second one-way hash function are the same one-way hash function.

21. (Currently Amended): The ~~system~~ method of claim 18, wherein the secure message comprises a protected message envelope, the method further comprising:

~~receiving a protected message envelope; and~~

~~generating a~~ extracting the random value, [[a]] the masked message, and [[a]] the first message validation code ~~based on~~ from the received protected message envelope.

22. (Currently Amended): A computer program product for secure communications in a message source, the computer program product having a computer readable medium with a computer program embedded thereon, the computer program comprising:

computer code for generating a random value;

computer code for generating a message validation code based on a message to be sent, the random value, a predetermined key, and a first one-way hash function;

computer code for generating a one-time pad based on the random value, the predetermined key, and a second one-way hash function;

computer code for generating a masked message based on the message to be sent and the one-time pad; [[and]]

computer code for generating a protected message envelope based on the random value, the masked message, and the message validation code; and

computer code for transmitting the protected message envelope to a message target,

wherein the message target is configured to unmask the masked message to form the message and validate the message using the message validation code.

23. (Currently Amended): A computer program product for secure communications in a message target, the computer program product having a computer readable medium with a computer program embedded thereon, the computer program comprising:

computer code for receiving a protected message envelope transmitted from a message source;

computer code for ~~generating~~ extracting a random value, a masked message, and a first message validation code based on the protected message envelope, wherein the

random value, the masked message, and the first message validation code are generated at the message source;

computer code for generating a one-time pad based on the random value, a predetermined key, and a first one-way hash function;

computer code for generating an unmasked message based on the one-time pad and the masked message;

computer code for generating a second message validation code based on the unmasked message, the random value, the predetermined key, and a second one-way hash function; and

computer code for comparing the first message validation code to the second message validation code to determine a validity of the unmasked message.